Augusta University / AU Health System

Cybersecurity Incident Response Policy

Policy Manager: Chief Information Security Officer

SCOPE

This policy clearly defines the roles and responsibilities necessary for the investigation of, and response to, cybersecurity incidents.

This policy applies to all Augusta University (AU) and AU Health information systems used to store, process, transmit or access electronic data as well as to all individuals who have access to these information systems including employees, students, contractors, those employed by contracted entities, and others authorized to access AU and AU Health enterprise technology assets and information resources.

POLICY STATEMENT

All users authorized to access AU and AU Health information systems and information technologies are responsible for promptly reporting any suspected or confirmed cybersecurity incidents involving Augusta University or AU Health data or information systems.

Reports are to be made via the Cybersecurity Incident Hotline or IT Service Desk.

- Cybersecurity Incident Hotline: 706-721-SAFE (7233)
- IT Service Desk: 706-721-4000

AFFECTED STAKEHOLDERS

Indicate all entities and persons within the Enterprise that are affected by this policy:

☒ AU staff, including permanent, temporary, and part-time
☒ AUHS, AUMC, AUMA, RWHS staff, including permanent, temporary, and part-time
☒ House staff, Residents, & Clinical Fellows
☒ Independent and Employed credentialed providers and Medical Staff
☒ Vendors/Contractors
☒ Researchers, students

☒ Any other individual with a relationship to AU or AU Health System that may create, use, disclose or access sensitive information

DEFINITIONS

Cybersecurity Incident: any suspected unanticipated or unauthorized action that has the potential to modify or change the confidentiality, integrity, or availability of sensitive information. Such examples could include: unconfirmed report of loss/theft of media that may contain sensitive information; potential unauthorized access of sensitive information via computer or network; unsubstantiated unauthorized or inappropriate use of another user's account or system privileges; any attempt to cause damage or harm to a system or network; or loss of records.

The **Chief Information Security Officer** is responsible for:

1. Developing and implementing a Cybersecurity Incident Response Plan that provides a well-defined and organized approach to handle any potential threat to information systems and electronic data and describes the roles and responsibilities of the Cybersecurity Incident Response Team

2. Establishing a Cybersecurity Incident Response Team responsible for the detection, categorization, reporting, containment, investigation, and mitigation of cybersecurity events, incidents, and/or policy violations

3. Initializing and leading the Cybersecurity Incident Response Team to ensure the Cybersecurity Incident Response Plan is put into action when a cybersecurity incident occurs

4. Notifying the President, Chief Information Security Officer, the University System of Georgia, and others of cybersecurity incidents per guidelines established in the Cybersecurity Incident Response Plan and the Board of Regents IT Handbook

5. Determining which individuals and functions should be assigned to manage the investigation process for each cyber security incident and policy violation

The **Cybersecurity Incident Response Team** is responsible for:

1. Detecting and investigating cybersecurity events to determine whether an incident has occurred, and the extent, cause and damage of incidents

2. Directing the recovery, containment and remediation of cybersecurity incidents, and may authorize and expedite changes to information systems as necessary

3. Coordinating response with law enforcement and/or external parties as determined by the Chief Information Security Officer and/or appropriate General Counsel

4. Monitoring relevant information systems as required, and retrieving/preserving data relevant to the cybersecurity incident investigation

The appropriate General Counsel(s) of both or either the University or the Health System and the Division of Communications & Marketing shall review and authorize any external disclosure of information regarding information security incidents.

The appropriate General Counsel(s) of both or either the University or the Health System shall lead communications with external authorities, including oversight and regulatory agencies.

APPROVED BY:

Executive Vice President for Academic Affairs and Provost, Augusta University
Date: 4/5/2019

President, Augusta University and CEO, AU Health System
Date: 4/5/2019